المحاضرة الثانية

الشبكات وفهم التهديدات الشبكية

يعد أمن الشبكات عنصرًا أساسيًا في حماية الأنظمة والمعلومات الحساسة من التهديدات المتزايدة. من خلال فهم أنواع التهديدات المختلفة وتطبيق أفضل الممارسات الأمنية، يمكن للأفراد والمؤسسات تقليل المخاطر وتحسين مستوى الأمان السيبراني لديهم. كما أن الاستثمار في التكنولوجيا الحديثة والتدريب المستمر يشكلان خط دفاع قوي ضد الهجمات الإلكترونية المتطورة.

1. مقدمة في أمن الشبكات

يشير أمن الشبكات إلى السياسات والتقنيات والممارسات المصممة لحماية الشبكات من الوصول غير المصرح به أو إساءة الاستخدام أو الأعطال أو خروقات البيانات. يضمن أمن الشبكات سلامة وسرية وتوافر مثلث الأنظمة والبيانات المتصلة بالشبكة.

1.1أهمية أمن الشبكات

- يمنع الوصول غير المصرح به وتسريبات البيانات.
- يحمي المعلومات الحساسة من مجرمي الإنترنت.
- يضمن أمان الاتصالات والمعاملات عبر الشبكة.
- يساعد في الحفاظ على توفر الأنظمة والخدمات بشكل مستمر.
- يقلل من المخاطر الناجمة عن الهجمات الإلكترونية الضارة.
- يساعد في الامتثال للقوانين واللوائح التنظيمية الخاصة بحماية البيانات.
- يحافظ على سمعة المؤسسات ويجنبها الخسائر المالية الناجمة عن الهجمات الإلكترونية.

1.2المفاهيم الأساسية في أمن الشبكات

- **السرية :(Confidentiality)** ضمان أن البيانات متاحة فقط للمستخدمين المصرح لهم.
- **السلامة :(Integrity)** ضمان بقاء البيانات غير متغيرة أثناء النقل أو المعالجة.
- **التوافر :(Availability)** ضمان توفر موارد الشبكة والخدمات عند الحاجة.
- **التوثيق :(Authentication)** التأكد من هوية المستخدمين المصرح لهم بالدخول إلى النظام.
- **التحكم في الوصول :(Access Control)** تقييد الوصول إلى الشبكة والمعلومات وفقًا لمستويات الصلاحية.
- **عدم الإنكار :(Non-repudiation)** ضمان عدم إمكانية إنكار العمليات التي تم تنفيذها على النظام.

2. فهم التهديدات الشبكية

2.1 أنواع التهديدات الشبكية

2.1.1 الهجمات البرمجية الضارة(Malware)

البرمجيات الخبيثة مصممة لإلحاق الضرر أو تعطيل النظام أو الوصول غير المصرح إليه.

- **الفيروسات :(Viruses)** برامج ذاتية النسخ تلتصق بالملفات.
- **الديدان :(Worms)** تنتشر عبر الشبكات دون تدخل المستخدم.
- **أحصنة طروادة :(Trojans)** تتنكر كبرامج شرعية لتنفيذ أنشطة ضارة.
- **برامج الفدية :(Ransomware)** تشفر الملفات وتطلب فدية لفك التشفير.
- **برامج التجسس :(Spyware)** تجمع بيانات المستخدم دون إذن.
- **البرمجيات الإعلانية الخبيثة :(Adware)** تعرض إعلانات غير مرغوب فيها وتجمع البيانات الشخصية.
- **بوت نت :(Botnet)** مجموعة من الأجهزة المصابة يتم التحكم بها عن بُعد لتنفيذ هجمات إلكترونية.

2.1.2هجمات التصيد والهندسة الاجتماعية

- **التصيد الاحتيالي :(Phishing)** انتحال شخصيات موثوقة لسرقة المعلومات الحساسة.
- **التصيد الموجه :(Spear Phishing)** هجوم تصيد موجه إلى فرد أو منظمة معينة.
- **التصيد عبر الرسائل النصية :(Smishing)** إرسال رسائل احتيالية عبر.SMS
- **التصيد عبر المكالمات الهاتفية :(Vishing)** الاتصال بالضحايا للحصول على معلومات حساسة.
- **الهجمات المعتمدة على الروابط الضارة :**إغراء الضحية بالنقر على روابط غير آمنة.

2.1.3هجمات حجب الخدمة (DoS) والهجمات الموزعة(DDoS)

- **هجوم حجب الخدمة :(DoS)** يغرق النظام بطلبات زائدة مما يجعله غير متاح.
- **هجوم حجب الخدمة الموزع :(DDoS)** يستخدم أنظمة مخترقة (بوت نت) لإغراق الهدف بحركة مرور زائدة.
- **HTTP Flood:**إرسال عدد كبير من الطلبات عبر HTTP لإرهاق الخادم.
- **SYN Flood Attack:**استغلال عملية المصافحة الثلاثية في TCP لإغراق النظام بطلبات غير مكتملة.
- **Ping of Death:**إرسال حزم بيانات كبيرة جدًا تتسبب في تعطيل النظام المستهدف.

2.1.4هجمات الرجل في المنتصف(MITM)

يتم اعتراض الاتصال بين طرفين للتنصت أو سرقة البيانات أو تعديل المعلومات.

- **التنصت السلبي :**قراءة البيانات دون تغييرها.
- **التنصت النشط :**اعتراض البيانات وتغييرها قبل إرسالها إلى الطرف المستهدف.
- **الهجمات على بروتوكول :HTTPS** استغلال الشهادات الرقمية الضعيفة لاعتراض الاتصالات المشفرة.

---

3. أفضل الممارسات لحماية الشبكات

3.1 حماية البنية التحتية للشبكات

- استخدام **الجدران النارية (Firewalls)** لمنع الاتصالات غير المصرح بها.
- تنفيذ **أنظمة كشف التسلل (IDS) ومنع التسلل.(IPS)**
- تطبيق **تشفير قوي للبيانات** أثناء الإرسال والتخزين.
- فصل الشبكات الداخلية عن الإنترنت باستخدام **نظام VPN آمن**.
- مراقبة **سجلات النظام (Logs Monitoring)** لاكتشاف الأنشطة المشبوهة.

3.2 السياسات الأمنية وإدارة الوصول

- استخدام **مصادقة متعددة العوامل (MFA)** لحماية الحسابات.
- تنفيذ **سياسات إدارة كلمات المرور** وتشجيع استخدام كلمات مرور قوية.
- فرض **مبدأ الأقل امتيازًا (Least Privilege Principle)** للحد من وصول المستخدمين إلى البيانات الحساسة.
- استخدام **التشفير التام بين الطرفين (End-to-End Encryption)** لحماية الاتصالات الحساسة.

3.3 التحديثات الأمنية والتدريب

- تحديث **البرمجيات والتطبيقات بشكل دوري** لتجنب استغلال الثغرات الأمنية.
- **تدريب الموظفين والمستخدمين** على تقنيات الهندسة الاجتماعية والهجمات الإلكترونية.
- إجراء **اختبارات أمنية دورية** وتقييم الأمان السيبراني للأنظمة.
- استخدام **تقنيات الذكاء الاصطناعي والتعلم الآلي** لاكتشاف الهجمات المحتملة.